

REMARKS

Reconsideration and allowance of the claims pending in the application are requested.

Claims 1-49 are pending in the application. as follows:

- 1) Claims 1, 2, 3, 4, 7-18, 19 and 20-37 and 49 have been rejected under 35 USC 103 (a) as unpatentable over Cofta, of record, in view of DiLuoffo et al., of record.
- 2) Claim 6 has been rejected under 35 USC 103 (a) as unpatentable over Cofta, of record, as modified by DiLuoffo et al., of record and US 2002/0131445 to Skubic et al.(hereafter, "Skubic et al."), published September 19, 2002.
- 2) Claims 5, 38-47 have been rejected under 35 USC 103 (a) as being unpatentable over Cofta, of record, as modified by Di Luoffo, of record and Skubic et al. in view of USP 6,587,835 to Treyz et al., of record.

Applicants' attorney thanks Primary Examiner Pierre Elisca and Examiner Evens Augustin for the courtesy of a telephonic interview conducted March 31, 2006. The interview discussed claims 1 and 37 and reviewed Word Document Number 70793 entitled "Sovio (SN 10/785,025) Vs Cited Art" (attached as Exhibit A) prepared by Applicants' attorney for purposes of distinguishing the subject matter of claims 1, 19, 37 and 6 from the cited art. The Document was provided to the Examiner prior to the Interview. Applicants' attorney noted the cited references, alone or in combination, failed to disclose or suggest (i) a pilot device or smart card which communicates with both a mobile device and a self service terminal via RFID connections, (ii) a mobile device transferring security information to a pilot and the pilot transferring the security information to the self service terminal via the RFID connections, (iii) the self service terminal using the security information to establish a RF connection with the mobile terminal, where the RFID connection to the self service terminal has a small range than the RF connection between the self service terminal and the mobile device, and (iv) the mobile device transferring security information to a master pilot device via a RFID connection for activating slave mobile devices for interacting with a self service terminal via a RFID connection. The Document demonstrated the cited art, alone or in combination, did not disclose or suggest the claimed subject matter. The Examiners indicated the claims did not clearly bring out the differences, and such clarification of the claims in an amendment to the subject Office Action would possibly overcome the rejection.

Before responding to the rejection, Applicants would like to distinguish Cofta, DiLuoffo, Skubic, and Treyz (the cited art) from the invention (Sovio), as follows:

A. Cofta communicates with a card issue via a mobile phone to obtain authorization information to purchase goods from a self service terminal and providing the authorization information to the terminal to complete the transaction. The Examiner acknowledges Cofta fails to disclose a portable pilot linked to a mobile phone.

B. DiLuoffo discloses a smart card attached or communicating with a mobile phone, the card containing security information enabling the mobile phone to conduct secure and non-secure transactions with a terminal. DiLuoffo fails to disclose (i) the smart card as a user carried fob or pilot for conducting transaction with a terminal, (ii) the smart card linked to both the mobile phone and a terminal, (iii) the smart card providing security information to the terminal from the mobile phone, and (iv) the terminal establishing a connection with mobile phone using the security information provided by the smart card

C. Skubic only discloses a Bluetooth connection between a terminal and a mobile phone for communication purposes. Skubic does not supply the missing features in Cofta and DiLuoffo, described above .

D. Treyz discloses a handheld computer or mobile phone interacting with a terminal at short RF ranges for conducting transactions with a terminal. Treyz fails to disclose the handheld computer linked to both a mobile phone and to a terminal and able to conduct transactions with the terminal based on security information received from the mobile phone.

E. The combination of the cited art does not teach or suggest to a worker skilled in the art a user portable fob or pilot linked to both a mobile phone and terminal, wherein (i) the fob or pilot uses security information provided by the mobile phone to conduct transactions with the terminal, (ii) after a connection is established between the terminal and mobile phone, (iii) based on security information provided to the terminal by the fob or pilot device.

Now turning to the rejection, Applicants responds to the indicated paragraphs of the Office Action, as follows:

Paragraphs 2/3:

Claims 1-4, 7- 37 and 49, after amendment, include features not disclosed or suggested in Cofta in view of DiLuoffo, and overcome the rejection under 35 USC 103 (a), as follows

A. Claim 1:

i) imprinting at least an association of the security key and mobile phone identification into at least one user portable fob or pilot via an initial short-range radio link ;

DiLuoffo does not supply the missing feature in Cofta. DiLuoffo discloses imprinting security information from a smart card to an attached or radio linked mobile phone, whereas applicants disclose the reverse, that is, imprinting security information from the mobile phone into the user portable fob or pilot.

ii) transferring at least the association of the security key and the mobile phone identification from the at least one user portable fob or pilot to a self-service merchant terminal through the initial short-range radio link;

DiLuoffo does not supply the missing feature in Cofta. DiLouffo does not disclose the smart card transferring mobile phone security information into the self service terminal

iii) establishing a secure short-range connection between the self-service terminal and the mobile phone based on the transferred security key and the mobile phone identification information from the at least one user portable fob or pilot, wherein the initial short-range radio link has a significantly smaller radio coverage than the secure short-range connection.

DiLuoffo does not disclose the missing feature in Cofta. DiLuffo fails to disclose (i) the smart card as a portable fob or pilot for conducting transaction with the terminal; (ii) providing security information to the self service terminal to enable the terminal to establish a short range connection with the mobile phone.

Summarizing, Cofta in view of DiLuoffo fails to disclose or suggest features (i), (ii), and (iii), described above. The rejection of claim 1 under 35 USC 103 (a) is without support in the cited art. Withdrawal of the rejection and allowance of Claim 1 are requested .

B. Claim 19:

(i) A system for enabling a user in a mobile environment to conduct transactions via a self-service terminal, comprising: a user portable fob or pilot device associated with the mobile device and including a semi-passive RFID transponder;

DiLuoffo discloses a smart tag communicating with a mobile device and fails to disclose a user portable fob or pilot for conducting transaction and including a RFID transponder.

ii) means for imprinting said stored identification and at least an association of the security information of the device over an RFID connection into the user portable fob or pilot;

DiLuoffo discloses the smart card imprinting security information into the mobile device whereas applicants imprint the mobile device security information into the user portable fob

iii) means for transferring by the user fob or pilot said imprinted identification and security information to the self-service terminal over an RFID connection; and

DiLuoffo fails to disclose the smart card transferring security information into the self-service terminal via an RFID connection.

iv) means for establishing a secure short-range connection between the self-service terminal and the device based on said transferred identification and security information of the device from the user portable fob or pilot, wherein the RFID connection has significantly smaller radio coverage than the secure short-range connection.

DiLuoffo fails to disclose the terminal using the information transferred from the user fob to set up a short range connection with the mobile device.

Summarizing, Cofta in view of DiLuoffo fail to disclose or suggest features (i) – (iv), described above. The rejection of claim 19 under 35 USC 103 (a) is without support in the cited art. Withdrawal of the rejection and allowance of Claim 19 are requested.

C Claim 27:

i) a user portable fob or semi-passive transponder for responding to RF signals transmitted by an associated mobile device;

DiLuoffo discloses a smart card or transponder providing signal to a mobile device, whereas applicants disclose a user portable fob or pilot receiving signals from a mobile device.

ii) means responsive to the transponder for storing unique information related to a mobile device.

DiLuoffo does not disclose storing unique information received from a related mobile phone.

Summarizing, Cofta in view of DiLuoffo fails to disclose or suggest features (i) and (ii), described above. The rejection of claim 27 under 35 USC 103 (a) is without support in the cited art. Withdrawal of the rejection and allowance of Claim 27 are requested.

D. Claim 33:

Claim 33 corresponds to claim 1, but written in product format. Claim 33 is patentable over the cited art for the same reasons indicated in connection with the consideration of claim 1.

E. Claim 37:

(i) A method of enabling a first user portable fob or pilot device to serve as a master pilot for at least one second user portable fob or pilot devices as slave devices capable of interacting with a terminal, comprising: installing a reader and switching means in the first user portable fob or pilot device serving as a master device and further including a processor and storage means;

DiLuoffo fails to disclose a user portable fob or pilot carried by the user and serving as a master device for second user portable fobs or pilot devices.

(ii) imprinting and storing in the master user fob or pilot device a phone address and a security key of a mobile phone;

DiLuoffo discloses the smart card imprinting the mobile device with security information, whereas applicants disclose the mobile device imprinting the user carried fob with security information.

(iii) At least one second user portable fob or pilot device, each serving as a slave device to the master device and further including a processor and storage, each slave device capable of receiving and transmitting signals from/to the master device;

DiLuoffo fails to disclose second user portable fob or pilot devices.

(iv) imprinting the phone address, security key and policy restraints by the master device in a slave device after receiving an address identifying the slave device; and

DiLuoffo fails to disclose a smart card imprinting slave devices with security information master.

(v) using the slave device to interact with a terminal to purchase an item, after a secure connection is established between the terminal and the mobile phone.

DiLuoffo fails to disclose smart cards interacting with a terminal to purchase an item.

F. Claims 2-4 and 7-37 depend from and further limit claim 1. Claims 2-4 and 7-37 are patentable over the cited art for the reasons indicated above in connection with the consideration of the cited art.

G. Claim 49:

Claim 49 combines claims 1, 7 and 16 and is patentable over the cited art on the same basis as claim 1.

Summarizing, Cofta in view of DiLuoffo fails to disclose or suggest features (i)- (v), described above. The rejection of claims 1-4, 7-37 and 49 under 35 USC 103 (a) is without support in the cited art. Withdrawal of the rejection and allowance of Claims 1-4, 7-37 and 49 are requested .

Paragraph 4:

Claim 6 includes features not disclosed in Cofta as modified by DiLuoffo in view of Skubic, and overcomes the rejection under 35 USC 103 (a), as follows:

Claim 6 depends from claim 1 is patentable over the cited art for the same reasons indicated in connection with the consideration of Claim 1. Withdrawal and allowance of Claim 6 are requested.:

Paragraph 5:

Claims 5, 38-47 include features not disclosed in Cofta, as modified by DiLuoffo and Skubic in view of Treyz, and overcome the rejection under 35 USC 103 (a), as follows

A. Skubic and Treyz do not supply the missing features in Claim 1, and not found in Cofta in view of DiLuoffo, as indicated above in the consideration of the cited art . Claim 5 depends from and further limit Claim 1. Claim 5 is patentable over the cited art for the same reasons indicated in connection with the consideration of Claim 1. Withdrawal of the rejection and allowance of Claim 5 are requested.

B. Skubic and Treyz do not supply the missing features in Cofta in Claims 27-48, and not found in Cofta in view of DiLuoffo, as indicated above in the consideration of the cited art. Claims 38 – 47 depend from and further limit Claim 37 . Claims 38-47 are patentable over the cited art for the same reasons indicated in connection with the consideration of claim 38.

CONCLUSION:

Having amended claims 1, 19, 27, 33, and 37 to further define and distinguished the claimed subject matter from the cited art, applicants request entry of the amendment; withdrawal of the rejection; allowance of the claims, and passage to issue of the case.

AUTHORIZATION

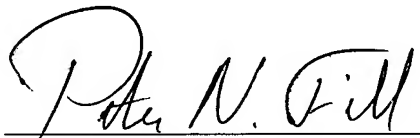
The Commissioner is hereby authorized to charge any additional fees which may be required for consideration of this Amendment to Deposit Account No. 13-4503, Order No. 4208-4169. A DUPLICATE OF THIS DOCUMENT IS ATTACHED.

In the event that an extension of time is required, or which may be required in addition to that requested in a petition for an extension of time, the Commissioner is requested to grant a petition for that extension of time which is required to make this response timely and is hereby authorized to charge any fee for such an extension of time or credit any overpayment for an extension of time to Deposit Account No. 13-4503, Order No. 4208-4169. A DUPLICATE OF THIS DOCUMENT IS ATTACHED.

Respectfully submitted,  
MORGAN & FINNEGAN, L.L.P.

Dated: April 27, 2006

By:

 38,876  
\_\_\_\_\_  
Joseph C. Redmond, Jr.  
Registration No. 18,753  
(212) 415-8700 Telephone  
(212) 415-8701 Facsimile

Correspondence Address:

MORGAN & FINNEGAN, L.L.P.  
3 World Financial Center  
New York, NY 10281-2101



## EXHIBIT A

Sovio (S.N. 10/785,025) Vs Cited Art

Claim	Sovio	Cofta	DiLuoffo	Skubic	Treyz
Claim 1	Filed 2/25/04	Filed 12/19/00	Filed 5/22/03	Filed 3/01	Filed 2/01
Method to Conduct Transactions in a Mobile Environment	<p>A short- range communication method, system and program product enable a user in a mobile environment to conduct short-range transactions with a self-service merchant terminal.... with respect to transaction security and payment mechanism without using currency</p> <p>Pg. 3, Lines 17-20.</p> <p>Fig. 1.</p>	<p>A system for performing a transaction, comprising a communications device (CD), a first party and a second party, (P9). CD may be a mobile phone (P69)</p>	<p>A smart card system for secure transmission of post issuance data to an embedded chip using a chip relay module, a plurality of hardware security modules.....(P10)</p>	<p>A method and apparatus for enabling anonymous communications from a first Bluetooth device to a second Bluetooth device wherein a temporary identification number associated with the first Bluetooth device is obtained and used in transmissions from the first Bluetooth device to the second Bluetooth device. (Abstract)</p>	<p>a cellular telephone with computing capabilities may be used to perform some of the functions of handheld computing device 12. For many functions, handheld computers may be preferable to cellular telephones. (Col. 9, Lines 60-65)</p>
Maintain Security Key in Mobile Device (MD)	<p>The phone includes an application for: (1) generating and sending the pilot a random nonce and a sequence number (SEQ), and (2) imprinting a secret key (k) and the phone address, typically the</p>	<p>Security Key maintained in SIM Card of CD. (P45)</p>	<p>Alternatively, card reader/writer 112 may be a reader only such as a cellular phone... (which) have dual slots where one slot is for SIM and the other slot is for the smart card.</p>		

	MAC address in the pilot via a RFID connection. Pg. 3, Lines 23-26.				
Imprint Security Key (SK) & MIN Into Portable Pilot	Figure 5 describes a generic process 600 for imprinting a secret key (k) and identification information, such as an address (typically a MAC address) of a phone or mobile device (as a Master) 601 into a pilot (slave) 603. Pg. 11, Lines 18-20.	PP not disclosed.	smart cards in use today are flat, rectangular pieces of plastic resembling credit cards having electronic circuitry embedded therein. A typical smart card includes a microprocessor coupled to a memory, and the microprocessor executes instructions and performs operations on data of at least one software application program stored in the memory. Smart cards commonly appear in the form of credit cards, key-shaped tokens, and subscriber identity modules (SIMs) used in certain types of cellular telephones. (P03)		
Transfer SK & MIN From Pilot to SS Term. via SR Radio Link	The pilot computes $RES = f(\text{nonce}, SEQ, k)$ (k is from imprinting) and $K' = g(\text{nonce}, SEQ, k)$ and sends these to the terminal as a response message, (f) and (g) being	Transfer of SK to Term. Via SR radio Link – <u>Not disclosed.</u>	When smart card 102 is inserted into card reader/writer 112, corresponding members of the two sets of contacts may come into physical contact with one another. Alternately, both card reader/writer 112 and smart		Wireless communications paths that use short-range optical connections such as IR links and short-range RF links over distances from a fraction of a foot to hundreds of feet are referred to herein as "local" communications paths or links. An

	one-way functions . based on cryptographic hash computations. Pg. 15, Lines 12-14.		card 102 may include wireless communication interfaces for communicating without electrical contact. In addition, card reader/writer 112 and smart card 102 are preferably capable of establishing and carrying out secure communications. (P96). <u>DiLuoffo fails to disclose a SR Radio Link.</u>		example of a local communications path is an IR link between handheld computing device 12 and a kiosk or cash register. Another example of a local communications path is a Bluetooth connection between handheld computing device 12 and a wireless transmitter/receiver. (Col. 13, Lines 2-38) <u>Treyz discloses IR links and SR connections and fails to disclose RFID connections.</u>
Establish SR connection (Cn) between SS Term. & MD where SR link has smaller radio coverage than SR Cn.	<p>The terminal uses session key K' to establish a secure short-range communication channel with the phone. The counter part, which is the phone, derives the session key K' and uses that for the secure communication. Pg. 15, Lines 15-17.</p> <p>The necessary information for the connection establishment is provided through the portable pilot by an initial short-range link between the self-service terminal and the</p>	Alternatively, the connection to the point of sale device can use .....For example, the "Bluetooth" proposed standard can be used. (P34) <u>SR link is not disclosed.</u>	<u>DiLuoffo fails to disclose a SR radio link and a SR Connection.</u>		<u>Treyz fails to disclose a SS terminal including RFID links and SR connections.</u>

	pilot, which has a significantly smaller radio coverage than the secure short-range connection to minimize the possibility of eavesdropping. Pg. 16, Lines 4-7.				
Claim 19					
System to Conduct Transactions in a Mobile Environment	Se Claim 1 above.	See Claim 1 above.	See Claim 1 above.		
MD incl. SR transceiver & RFID transceiver	Pg. 9, lines 17-20.	The communication device 22 may be a mobile telephone..... arranged solely to communicate with the point of sale devices 16 and the card issuer 12.(P24). <u>RFID transceiver not disclosed.</u>	DiLuoffo fails to disclose SR transceiver and RFID transceiver.		
Portable Pilot (PP) incl. semi-passive RFID transponder	Pg. 10, Lines 11-30.	<u>Not Disclosed</u>	<u>Not Disclosed</u>		
A SS Term. Including RFID Transc & SR Transc	Pg. 11, Lines 15-17.	Alternatively, the connection to the point of sale device can use .....For example, the "Bluetooth" proposed standard can be used (P34). <u>Cofta fails to</u>	Alternately, both card reader/writer 112 and smart card 102 may include wireless communication interfaces for communicating without electrical contact. (P96). <u>DiLuoffo fails to</u>		

		<u>disclose two different transceivers in the Terminal</u>	<u>disclose a RFID transceiver and a SR transceiver.</u>		
Means Storing Id Inf. & Sec. Inf. In MD	Pg. 9, Lines 18-28.	The authentication centre of the network generates a random number and secret key are used in a manner..... which verifies the identity of the .. device 22. (P45) <u>Cofta fails to disclose Id in MD.</u>	smart card 102 includes a chip identification number (CIN) 400. Following authentication of the user, CRM ....requests CIN 400 from smart card 102 and smart card 102 responds by providing CIN 400 to computer system 110. <u>DiLuoffo fails to disclose imprinting stored Id &amp; Sec. Info. Into MD.</u>		
Means imprinting stored Id & Sec. Inf. Into PP	Pg. 1, Lines 18-29.	<u>PP not disclosed.</u>	<u>DiLuoffo fails to disclose imprinting stored Id &amp; Sec. Info. Into smart card.</u>		
Means transferring by PP imprinted Id & Sec Inf. to SS Term via RFID connection	Pg 15, lines 1-3.	<u>PP &amp; RFID connection not disclosed.</u>	<u>DiLuoffo fails to disclose transferring by smart card imprinted Id &amp; Sec. Info into SS Terminal via RFID connection.</u>		
Means Establishing Secure SR Conn. between SS Term & MD where RFID conn. has smaller radio coverage the SR Conn.	Pg. 15, Lines 4-17.	<u>RFID connection not disclosed.</u>	<u>RFID connection not disclosed.</u>		
Claim 37					
Method enabling First PP to serve as a Master PP for at least	See Claim 1 above.	See Claim 1 above.	See Claim 1 above.		

One Slave PP capable of inter acting with a Term.					
Installing Reader & switch in First PD incl. a Processor & Storage & serving as a Master PD (MPD)	Pg. 13, Lines 2-6.	<u>MPD not disclosed.</u>	<u>Master smart card not disclosed.</u>		
Imprinting & Storing in MPD phone address & SK of a mobile phone	Pg. 13, Lines 7-21.	<u>MPD not disclosed.</u>	<u>Master smart card not disclosed.</u>		
At least one second PD serving as a slave device (SD) & further incl. a Processor & Storage, each slave device capable of receiving & transmitting signals from MPD	Pg. 13, Line 9.	<u>SD not disclosed.</u>	<u>Slave smart card not disclosed.</u>		
Imprinting phone address, SK & policy restraints in slave after receiving an address identifying the slave device	Pg. 13, Lines 7-21.	<u>SD not disclosed</u>	<u>Master smart card not disclosed.</u>		
Using the slave device to interact with a Terminal to purchase an item, after a secure connection is	After the establishment of the secure connection, the holder of the slave fob interacts with the self-service terminal to	<u>SD not disclosed.</u>	<u>Slave Device not disclosed.</u>		

established between the Terminal & the mobile phone.	make purchases according to a shopping list, A clerk at the counter delivers the purchased items. Pg. 13, Line 22 continuing to Pg. 14, line 3.				
Claim 6					
The method of Claim 1, wherein the mobile phone identification is a Bluetooth address of the mobile phone.	a secure short-range connection between the self-service terminal and the mobile phone, wherein the pilot 703 simply provides the self-service terminal 701 with phone address 705 (Bluetooth address of the mobile phone). Page 15, Lines 23-25.			a Bluetooth radio unit transmits over the wireless link a unique identity number that enables other devices to identify and address the Bluetooth radio unit. (P02)	